Statement of
Steven I. Cooper
Chief Information Officer
Department of Homeland Security

before the

Committee on Government Reform
House of Representatives
May 8, 2003

Mr. Chairman and Members of the Committee:

I am pleased to appear before the Committee today to discuss information integration at the Department of Homeland Security (DHS). First, I want to thank the Chairman and the other members of the Committee for your leadership in the strategic use of information technology in the federal government and in homeland security. These strategic investments will improve the performance and accountability of the federal government as a whole, and homeland security, specifically. Information is a vital foundation for the Department's operations and consequently for improving our Nation's homeland security.

I have served as the Chief Information Officer (CIO) for DHS since its inception January 24, 2003. In this role, I provide strategic direction and oversight for information technology programs within DHS. From February 2002 until the formation of DHS, I served as a Special Assistant to the President and Senior Director for Infrastructure Integration for the White House Office of Homeland Security.

The *National Strategy for Homeland Security* set forth a vision to mobilize and organize our Nation to secure the U.S. homeland from terrorist attacks. This document identified three strategic objectives of homeland security:

- Prevent terrorist attacks within the United States;
- Reduce America's vulnerability to terrorism; and
- Minimize the damage and recover from attacks that do occur.

As stated in the *National Strategy*, although American information technology is the most advanced in the world, our country's information systems have not adequately supported homeland security missions. Databases used for law enforcement, immigration, intelligence, public health surveillance, and emergency management have not been integrated in ways that allow us to comprehend each other's data or "connect the dots" to better prevent terrorist attacks and protect our people and infrastructure from terrorism. Technologies and cultures of agencies have to "Islands of Technologies" and barriers to information integration. We must leverage cultural beliefs and diversity to achieve

collaborative change while at the same time consolidating redundant or duplicative efforts. In addition, there are deficiencies in the communications systems used by Federal, State and Local entities, and most state and local first responders do not use modern, compatible wireless communications equipment. To secure the homeland better, we must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy.

Information Sharing is a key foundation that cuts across all mission areas, all levels of government, and all sectors of our society. The *National Strategy for Homeland Security* identifies five major initiatives:

- Integrate information sharing across the federal government;
- Integrate information sharing across state and local governments, private industry, and citizens;
- Adopt common "meta-data" standards for electronic information relevant to homeland security;
- Improve public safety emergency communications; and
- Ensure reliable public health information.

We must put in place mechanisms that provide the right information to the right people in a timely manner.. With the use of information technology, homeland security officials throughout the United States will have a more complete, common awareness of threats and vulnerabilities as well as knowledge of those personnel and resources that are available to conquer those threats. Officials will receive actionable information they need from all levels of government and the private sector so that they can anticipate threats and respond rapidly and effectively. This information integration will better enable officials to protect the physical and cyber infrastructure, secure our country's borders, prevent biological or chemical attacks, and provide an effective first response to a terrorist or natural disaster incident.

Our vision is to ensure a world-class information management infrastructure that provides
timely, accurate, useful, and actionable information to all individuals who require it.

This strategy and vision will be enabled by a disciplined **capital planning and investment control process** guided by a business-driven **enterprise architecture**.

INVESTMENT REVIEW PROCESS

In July 2002, under direction of the Office of Management and Budget in consultation with the White House Office of Homeland Security, an Information Technology Review group was formed to review all IT investments over $500,000 for infrastructure or business applications by agencies that had been identified to move into the proposed Department of Homeland Security. This early start at investment review allowed early

implementation of decisions to foster a migration from "bureau-centric" investments to "Department-level" investments. Actions to date have saved over $20 M, due to three Enterprise-wide software agreements.

With the formation of DHS in March 2003, information technology investments, including mission-specific investments, are now receiving a department-wide review. Information integration will be one of the benefits of the capital planning and investment and control process. Each investment is reviewed to ensure alignment with business process, consistency with technical frameworks and standards, and use of DHS-wide "meta data". This review process will identify and eliminate duplication of applications, gaps in information or misalignment with business goals and objectives.

ENTERPRISE ARCHITECTURE

In July 2002, we began to develop a business-driven Homeland Security Enterprise Architecture. Architecture working groups were established to collect, organize and publish the "as is" architecture for the major components proposed to come to DHS. Using this baseline information, we developed harmonized concepts of operation for use by DHS transition teams. The "as is" architecture for DHS is about 70 % complete. An inventory of "as is" applications is also about 70% complete. This inventory contains approximately 100 major applications and over 2,000 IT applications. The final DHS "as is" architecture and inventory will be completed in June 2003. During the process, the technical reference model for each DHS component will be collected, compared and evaluated. Information technology solutions will be grouped into the following categories: Nearly 100% commonality; roughly 80% commonality; and little commonality.

Analysis has already led to--

- Enterprise-wide software licensing efforts within the department, linked to the President's E-Government initiative across the federal enterprise;
- Identification of areas where a common technical solution could be rapidly selected and deployed; and
- Identification of instances where additional analysis is needed before enterprise technical solutions are possible.

The "to be" DHS architecture will be developed over this summer based on the business strategies of the DHS mission elements and on information technology opportunities. The initial "to be" architecture will be completed in August 2003.

Once we have formulated our "to be" architecture, we can develop the migration strategy needed to move from where we are today to where we want to be as a department. We plan to develop a plan, or road map, that provides a phased approach to achieving the "to be" architecture by fall 2003. We plan to initiate a competitive procurement in May 2003 for support of this architecture effort.

To better address horizontal information integration, DHS has coordinated its enterprise architecture development with other key Federal agencies, including the Departments of Justice, Energy and Defense, and the Intelligence Community. To address vertical information integration, DHS included National Association of State and Local CIOs (NASCIO) in our architecture development efforts through several coordination workshops. These relationships will continue during the development of the "to be" architecture and as we execute our roadmap.

INFORMATION TECHNOLOGY PRINCIPLES

We developed a modest set of information technology principles to both guide our initial investment decisions and our development of the "to be" enterprise architecture vision. Some of these principles reflect best practices successfully used in both industry and government. A few key principles include--

1. A proper balance of security and privacy. Implementations must ensure adequate and appropriate protection of legal civil liberties, and processes must be established to ensure information is accurate and privacy is protected. At the same time, information integration must be exploited to significantly improve our nation's homeland security.
2. Information systems should be built once and re-used within other DHS domains. Information should be captured once and re-used for multiple purposes.
3. The strategic, operational and governance activities of the department's Information Technology functions should be organized to ensure alignment with the business strategies of the department and its organizational elements.
4. Information Technology functions should use a balanced scorecard to guide and measure progress among and across the IT function.
5. Data and information generated by the department's organizational elements are the property of the department. These assets will be secure and available to those who have a legitimate need to use them.
6. We will deploy solutions that maximize value in support of mission and department objectives, using commercial off-the-shelf products and software wherever possible.
7. We should adopt common meta-data standards for homeland security information within DHS and promote common meta-data standards among key federal, state, local, and industry partners.
8. We should embrace open standards and non-proprietary approaches whenever possible.

INITIATIVES IN INFORMATION SHARING

Several key information-sharing initiatives have been initiated to address critical homeland security information sharing needs.

Events of September 11, 2001, reinforce the need to share and provide actionable information. "Watch" lists contain information on terrorists that support a variety of homeland security missions. As part of the transition process, we began to identify and begin the integration of "watch" lists within the Federal government. Eleven lists were identified in the "as is" inventory. Virtually all lists derive from one database. A plan to improve the dissemination of information from this database at three levels of classification has been developed, including a concept of operations, phasing and technical approach. Clearly we need to work with the other federal agencies involved with watch lists to address possible issues of redundancy and duplication.

In March 2003, a policy and technical framework to promote information sharing among the Department of Justice, the Intelligence Community and the Department of Homeland Security was completed that provides a framework for implementing an integrated "watch" list. Additionally, in collaboration with the Department of Justice, DHS has supported the extension of law enforcement information sharing networks such as the Regional Information Sharing Network (RISSNET) to provide a distribution channel for law enforcement homeland security information.

In another project, DHS has been working with "best of breed" regional information sharing groups such as the Emergency Response Network of Dallas, Texas (ERN), to provide homeland security information to a broad cross-section of first responders. We have connected the Department's Homeland Security Center to the ERN as a pilot for information exchange with State and Local governments, and with private sector critical infrastructure.

The Emergency Preparedness and Response component of DHS is providing secure video conference capability to governors and emergency response centers for each of the 56 states, territories or protectorates. These videoconference capabilities will support communication and information sharing of sensitive information with the states and territories. DHS is also the managing partner for the Disaster Management E-Gov Initiative, a Presidential Management Agenda program designed to provide an easy to use, unified point of access to disaster management knowledge and services. The program has a portal, tools for responders, and an interoperability backbone.

Utilizing lessons learned from the private sector on the importance of communication, DHS has implemented a single external portal, and a single internal portal, to provide for effective and consistent communications external to DHS and also internally to DHS employees. In addition, with little lead time, DHS has deployed DHS desktop server and office environments for all DHS Headquarters personnel. We are implementing a secure intranet to all 170,000 DHS employees with a single "meta" directory for all DHS employees. The intranet provides all DHS employees with access to the internal portal and collaboration suite of tools and the ability to receive and send e-mail messages with the simple dhs.gov address.

INFORMATION SHARING STRATEGY

Major objectives of our information sharing strategy include--

- Successful delivery of major Departmental IT initiatives. Information sharing will be achieved through data consistency (shared definitions of basic business objects such as "person" or "incident"). The DHS/CIO is supporting development of standardized data definitions to enable effective information sharing.
- Aggressive identification of opportunities for enterprise solutions and infrastructure investments at the department level. Examples include Targeting, Case Management, Intelligence Analysis, Infrastructure, Financial, Human Resource Management, Portal and Content Management, Geospatial, and Smartcard/Authentication.
- Information technology investments will be evaluated and managed using a balanced scorecard. Balanced scorecards are a strategic tool for managing IT projects, enabling the translation of mission and strategy into tangible objectives and measures using common, shared definitions, tools, and products. IT projects submitted to DHS require the inclusion of balanced scorecards. The four perspectives of the DHS balanced scorecard ensure we meet our mission strategy and align our IT functions:

  - *Customer:* Focuses on identifying the customer and measures associated with value provided to the customer, customer satisfaction, etc.
  - *Financial:* Focuses on readily measurable economic consequences of actions already taken.
  - *Internal Business Process:* Focuses on the internal processes that will have the greatest impact on customer satisfaction and achieving the business unit's financial objectives.
  - *Learning and Growth:* Focuses on the people, systems, and organizational procedures that are critical to building long-term organizational growth and improvement.

CONCLUSION

DHS remains in the early stages of the development of its enterprise architecture and use of capital planning and investment control. Even now though, and clearly into the future, these tools are being used to guide the development of DHS and the related foundational effort associated with information integration. DHS is committed to using the enterprise architecture to guide information sharing investment decisions.

We offer four final observations for your consideration:

- First, information sharing is fundamental to the achievement of homeland security mission.
- Second, DHS will aggressively develop and use a capital planning and investment control process to guide information integration investments.

- Third, DHS will aggressively develop and use a "to be" enterprise architecture to guide information integration efforts.
- Fourth, DHS will continually strive to be one unified department and resist compartmentalization.

There is significant momentum in the DHS for the use of enterprise architectures to promote information integration. With the support of the Congress, this momentum can be sustained and will help ensure that enterprise architectures play a major role in improving the performance and accountability of IT investments at both the department and government-wide levels.